ESCOLA DE GUERRA NAVAL

CC (T) Jane da Silva Pereira Azevedo

POSSIBILIDADES E LIMITAÇÕES DE EMPREGO DA GUERRA CIBERNÉTICA NA MB: IMPORTÂNCIA DOS EXERCÍCIOS NO ESPAÇO CIBERNÉTICO

Rio de Janeiro

2020

CC (T) Jane da Silva Pereira Azevedo

POSSIBILIDADES E LIMITAÇÕES DE EMPREGO DA GUERRA CIBERNÉTICA NA MB: IMPORTÂNCIA DOS EXERCÍCIOS NO ESPAÇO CIBERNÉTICO

Monografia apresentada à Escola de Guerra Naval, como requisito parcial para a conclusão do Curso Superior.

Orientador: CF (RM1) Fabiano Rabello Cantarino

Rio de Janeiro
Escola de Guerra Naval
2020

AGRADECIMENTOS

Agradeço a Deus em primeiro lugar, por me dar força, sabedoria e equilíbrio para enfrentar os momentos difíceis.

Aos meus pais, Paulo e Maria Dulce, pela minha formação.

Ao meu esposo Fábio e as minhas filhas Júlia e Luiza, pela compreensão, paciência e por estarem ao meu lado ao longo desta caminhada.

Ao Comandante e ao Chefe do Estado-Maior da minha Organização, respectivamente, Vice-Almirante Sergio Fernando de Amaral Chaves Junior e Capitão de Mar e Guerra Carlos Marden Soares Pereira da Silva, pela compreensão ao longo do curso.

Ao Capitão de Mar e Guerra (T) Antônio Carlos Pereira Borge, pela cooperação para o aperfeiçoamento deste trabalho.

Ao meu orientador, Capitão de Fragata (RM1) Fabiano Rabello Cantarino, por suas valorosas observações e contribuições, de forma objetiva e profissional.

Por fim, aos amigos do C-Sup/2020, em especial àqueles que fazem parte da turma do CFOF/2003, pelo companheirismo demonstrado durante todo o curso.

Se você conhece o inimigo e conhece a si mesmo, não precisa temer o resultado de cem batalhas. Se você se conhece, mas não conhece o inimigo, para cada vitória ganha sofrerá também uma derrota. Se você não conhece nem o inimigo nem a si mesmo, perderá todas as batalhas.

(Sun Tzu)

RESUMO

O amplo espectro de possibilidades de ações que podem ser empregadas no Espaço Cibernético requer especial atenção à segurança e à defesa desse domínio. Acompanhado de todas as facilidades e benefícios, esse ambiente se não protegido, pode ser comprometido por ameaças que buscam e exploram, a todo momento, possíveis vulnerabilidades existentes. Dessa forma, a proteção do Espaço Cibernético e, em especial das infraestruturas críticas de interesse nacional interligadas neste espaço, é fundamental para assegurar o seu uso efetivo pela sociedade. O Espaço Cibernético da Marinha do Brasil, composto por equipamentos interligados em que são trafegados seus ativos informacionais, também é considerado alvo das ações maliciosas de exploração e ataque cibernéticos. Destarte, são necessárias medidas que busquem o incremento da segurança dos sistemas de informação e das infraestruturas críticas de interesse no âmbito nacional e para a Marinha. Nesse contexto, propôs-se analisar as possíveis contribuições da realização dos exercícios de defesa no Espaço Cibernético realizados em outros países e no âmbito do Ministério da Defesa, assim como verificar a sua aplicabilidade para o Espaço Cibernético da Marinha. O embasamento teórico utilizado para a pesquisa consolidou-se no entendimento da estrutura do setor cibernético brasileiro que se concretizou para o cumprimento de ações estratégicas nacionais. Outrossim, foram analisados os exercícios cibernéticos identificados na literatura e observado o estreito relacionamento do exercício no âmbito nacional com a norma de Estratégia Nacional de Segurança Cibernética que possui como escopo a proteção das infraestruturas críticas nacionais. Conclui-se que, desde o momento em que o Espaço Cibernético foi considerado um domínio estratégico, muitos países já realizavam esse tipo de exercício. Mediante a análise dos exercícios pesquisados observou-se que eles refletiam a oportunidade para identificar fragilidades e a necessidade de melhorias nos processos e procedimentos até então implementados, além de fomentar o espírito de cooperação e integração entre os participantes. Não obstante, destacou-se que a realização dos exercícios cibernéticos, em âmbito nacional, contribuíram para superar alguns desafios elencados no trabalho e que poderiam incrementar o fortalecimento da Segurança e Defesa Cibernética do Espaço Cibernético da Marinha do Brasil.

Palavras-chave: Espaço Cibernético. Infraestruturas críticas. Exercícios no Espaço Cibernético. Segurança e Defesa Cibernética.

LISTA DE ABREVIATURAS E SIGLAS

AE	Ações Estratégicas
APF	Administração Pública Federal
CCDCOE	Cyber Defense Centre of Excellence
CGI.br	Comitê Gestor da Internet no Brasil
CIA	Agência Central de Inteligência
CLTI	Centros Locais de Tecnologia da Informação
ComDCiber	Comando de Defesa Cibernética
COTEC-TI	Comissão Técnica de Tecnologia da Informação
CSIRT	Computer Security Incident Response Team
CTF	Capture The Flag
CTIM	Centro de Tecnologia da Informação da Marinha
DCTIM	Diretoria de Comunicações e Tecnologia da Informação da Marinha
DE	Diretoria Especializada
DGMM	Diretoria-Geral do Material da Marinha
EB	Exército Brasileiro
ECIBER	Espaço Cibernético
ECIBER-MB	Espaço Cibernético da Marinha do Brasil
E-Ciber	Estratégia Nacional de Segurança Cibernética
EMCFA	Estado-Maior Conjunto das Forças Armadas
END	Estratégia Nacional de Defesa
FA	Forças Armadas
GC	Guerra Cibernética
GSI/PR	Gabinete de Segurança Institucional da Presidência da República
ITU	União Internacional de Telecomunicações
OM	Organização Militar
ONU	Organização das Nações Unidas
OTAN	Organização do Tratado do Atlântico Norte
PDN	Política de Defesa Nacional
PNSI	Política Nacional de Segurança da Informação
RECIM	Rede de Comunicações Integradas da Marinha

SIC	Segurança da Informação e Comunicações
SISMC	Sistema Militar de Comando e Controle
SMDC	Sistema Militar de Defesa Cibernética
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicações

SUMÁRIO

1 INTRODUÇÃO 8

2 ESTRUTURA CIBERNÉTICA NO ÂMBITO DO MINISTÉRIO DA DEFESA 10

2.1 Sistema Militar de Defesa Cibernética (SMDC) 10

2.2 As Ações Cibernéticas 12

2.3 Estrutura do Espaço Cibernético da MB 14

2.4 Infraestruturas Críticas 15

3 EXERCÍCIOS NO ESPAÇO CIBERNÉTICO — ECIBER 15

3.1 A identificação dos Exercícios Cibernéticos na Literatura 17

3.2 Exercício Cibernético no âmbito do MD 20

4 CONTRIBUIÇÕES PARA A SEGURANÇA E DEFESA CIBERNÉTICA 22

4.1 Identificação das contribuições resultantes da realização dos Exercícios Cibernéticos 23

4.1.1 A capacitação e o aprimoramento dos processos de tomada de decisão 23

4.1.2 O aprimoramento da capacidade de resposta e tratamento a incidentes de segurança 23

4.1.3 O aprimoramento do arcabouço normativo 24

4.1.4 O fortalecimento da proteção das infraestruturas críticas 25

4.1.5 O fomento à cooperação e integração nacional e internacional 25

4.2 Os Desafios a serem superados no âmbito nacional 26

4.2.1 Educação 27

4.2.2 Resposta aos incidentes e proteção das infraestruturas críticas 28

4.2.3 Cooperação e Integração 28

4.3 Identificação das contribuições dos Exercícios Cibernéticos para a SIC na MB 29

5 CONCLUSÃO 31

REFERÊNCIAS 33

ANEXO 35

1 INTRODUÇÃO

A atual conjuntura, caracterizada por incertezas, mutabilidade e volatilidade das ameaças cibernéticas[1], fazem com que a sociedade e, em particular, a expressão militar do Poder Nacional, precise estar permanentemente preparada. Para tal, medidas devem ser adotadas de forma a capacitá-la a responder oportuna e adequadamente aos possíveis cenários adversos à Defesa Nacional e à melhoria constante dos processos de Segurança das Informações e Comunicações (SIC), defesa e guerra cibernética.

No âmbito nacional, os sistemas da administração pública são considerados alvos atraentes quando são realizadas ações de explorações e de ataques cibernéticos. Essas ações são empregadas com o objetivo de causar diferentes impactos, tais como, dano à imagem dos órgãos governamentais perante a sociedade e o descrédito da população nos serviços prestados por esses órgãos.

Além da relevante necessidade da proteção desses sistemas, outro fator crítico refere-se à proteção dos sistemas afetos às infraestruturas críticas de interesse do País, relacionadas diretamente à segurança nacional.

Para alcançar a proteção das infraestruturas críticas de interesse e buscar o fortalecimento da segurança e defesa cibernéticas nacionais, atividades com abordagens mais sólidas e evolutivas devem ser implementadas no âmbito da Administração Pública Federal (APF), do Ministério da Defesa (MD), das Forças Armadas (FA), bem como no âmbito das instituições privadas e acadêmicas.

Nesse sentido, como no âmbito nacional, o Espaço Cibernético[2] de interesse da Marinha do Brasil (ECIBER-MB), composto por ativos de informação conectados em redes onde as informações digitais transitam, são processadas e armazenadas, também está sujeito a ações exploratórias e de ataques cibernéticos, por diferentes atores e com motivações diversas. Dessa forma, existe igualmente a necessidade constante do incremento dos processos e procedimentos para garantir um melhor nível da segurança desses ativos e das infraestruturas críticas da Força.

Os exercícios no Espaço Cibernético (ECIBER) consistem em atividades executadas em vários países há algum tempo e, que recentemente, passaram a ser empregados

---

[1] Ameaça Cibernética — causa potencial de um incidente indesejado, que pode resultar em dano ao Espaço Cibernético de interesse.

[2] Espaço Cibernético — espaço virtual, composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam, são processadas e/ou armazenadas.

e conduzidos no âmbito do MD. Os exercícios, conforme o escopo em que serão realizados, podem ter como objetivo identificar o nível de maturidade da segurança em que se encontra o ambiente, exercitar os processos decisórios em diferentes níveis de responsabilidade quando o ambiente estiver sofrendo ações que comprometam os requisitos de segurança e aprimorar a capacitação dos elementos participantes.

Com foco nesse contexto, surge a questão: os exercícios cibernéticos podem contribuir para o fortalecimento da Segurança e da Defesa Cibernética do ECIBER-MB?

Assim sendo, o objetivo geral deste estudo é identificar possíveis contribuições que a realização dos exercícios no espaço cibernético pode trazer para o incremento da segurança e defesa cibernéticas nacionais, assim como para a Segurança da Informação e Comunicações do espaço cibernético da MB. Para fundamentar o alcance desse objetivo, com um encadeamento lógico do raciocínio, foram delimitados os seguintes objetivos específicos: a) identificar a organização e a estrutura cibernética nacional; b) analisar a estrutura do espaço cibernético da MB; c) analisar a necessidade de proteção das infraestruturas críticas de interesse; d) identificar na literatura o conceito e a realização, em âmbito internacional e nacional, dos Exercícios Cibernéticos; e) analisar as contribuições resultantes da realização desses Exercícios Cibernéticos; e f) identificar os desafios a serem superados no âmbito nacional.

Este trabalho foi elaborado utilizando-se a pesquisa bibliográfica, investigando o problema a partir do referencial teórico existente em livros, leis, normas, doutrinas, artigos acadêmicos e sítios da Internet.

Visando orientar a leitura e facilitar a percepção do raciocínio da pesquisa realizada, este trabalho está dividido em cinco seções, iniciando-se por esta Introdução, que busca a apresentação dos aspectos abordados.

Na segunda seção, será apresentada a estrutura do setor cibernético no âmbito do MD e da MB, assim como os conceitos relacionados às ações cibernéticas e as infraestruturas críticas de interesse.

Na terceira seção, será apresentado o ECIBER como um novo domínio operacional afeto à defesa e segurança nacional. Assim como, serão identificados o conceito e a realização dos Exercícios Cibernéticos nas literaturas pesquisadas.

Na quarta seção, serão apresentadas as análises das contribuições resultantes da realização dos Exercícios Cibernéticos citados, assim como, a possibilidade da realização dos exercícios contribuírem para o fortalecimento da SIC na MB. Também na seção serão identificados alguns desafios a serem superados no âmbito nacional.

Finalmente na quinta seção serão apresentadas as conclusões da pesquisa, sobre os assuntos abordados, relacionados à evolução do setor cibernético e a execução dos exercícios no espaço cibernético.

2 ESTRUTURA CIBERNÉTICA NO ÂMBITO DO MINISTÉRIO DA DEFESA

Três setores tecnológicos são essenciais para a Defesa Nacional, dentre eles, destaca-se o cibernético. Em dezembro de 2008, a Estratégia Nacional de Defesa (END), aprovada por meio do Decreto nº 6.703, de 18 de dezembro de 2008, estabeleceu o setor cibernético como um setor estratégico, que requer estreita coordenação e integração de diversos atores e áreas de conhecimento. Conforme a minuta da END, apresentada no ano de 2016 para aprovação, a responsabilidade por este setor foi atribuída ao Exército Brasileiro (EB), ficando este com o desafio de buscar o aprimoramento da Segurança da Informação e das Comunicações e abrangendo a Segurança Cibernética, com ênfase na proteção das estruturas estratégicas afetas à Tecnologia da Informação (TI); bem como com a coordenação e integração das ações cibernéticas no âmbito das Forças Armadas (FA) (BRASIL, 2012a).

O setor cibernético no Brasil vem se estruturando, nos últimos anos, por meio de políticas, doutrinas, normatizações e centralização da sua coordenação. Com o tempo, surgiu um grande arcabouço normativo sobre este tema, permitindo um maior entendimento sobre esta nova dimensão. Dentre as diversas normas e políticas criadas para atender esse assunto, cabe destacar a aprovação por parte do MD, em 2012, da Política Cibernética de Defesa (BRASIL, 2012), que estabelece as diretrizes para a Defesa Cibernética do País, tendo a finalidade de orientar, no âmbito do MD, as atividades de Defesa e Guerra Cibernética (GC), nos níveis estratégicos, operacional e tático. Nessa Política, destacam-se diretrizes para assegurar o uso efetivo do espaço cibernético, de forma conjunta, pelas FA e para impedir ou dificultar a sua utilização por interesses que vão contra aos da Defesa Nacional. Além disso, este documento contribuiu para a concepção e implantação do Sistema Militar de Defesa Cibernética (SMDC) que, atualmente, conta com a participação de militares das FA e civis (BRASIL, 2012c).

2.1 Sistema Militar de Defesa Cibernética (SMDC)

Conforme definido na END, por ser um dos componentes da Defesa Nacional, a Defesa Cibernética é missão das FA. Porém, o cumprimento desta missão se torna bastante difícil se não houver a atuação colaborativa da sociedade brasileira, imbuída do sentimento de

responsabilidade individual e coletiva pela proteção das infraestruturas críticas[3] (BRASIL, 2014, p. 25).

As atividades de Defesa Cibernética devem ser orientadas para atender às necessidades da Defesa Nacional. Com a finalidade de facilitar as ações necessárias quando do momento de transição da situação de normalidade para a situação de crise ou conflito, o MD busca priorizar a integração com órgãos de interesse.

Dentro desse contexto, nasceu o SMDC, contando com a participação de militares das FA e civis. Conforme apresentado na FIG. 2 do ANEXO, o SMDC é formado por um conjunto de doutrinas, procedimentos, tecnologias e pessoal essenciais voltado para a realização das atividades de defesa no espaço cibernético, assegurando, de forma conjunta, o seu uso efetivo pelas FA; bem como para impedir ou dificultar a utilização desse espaço contra os interesses da Defesa Nacional. Cabe ao SMDC assegurar a proteção cibernética do Sistema Militar de Comando e Controle[4] (SISMC), assim como coordenar e integrar a proteção das infraestruturas críticas de interesse definidas pelo MD (BRASIL, 2014, p. 26).

Atualmente, o órgão central do SMDC é o Comando de Defesa Cibernética (ComDCiber), que atua sob a orientação e supervisão do Estado-Maior Conjunto das Forças Armadas (EMCFA), subordinado ao Comando do Exército, realizando ações de coordenação e integração com os setores cibernéticos das FA e com órgãos de interesse envolvidos nas atividades de Defesa Cibernética. De acordo com a FIG. 2 do ANEXO, a estrutura definida do SMDC viabiliza a coordenação entre agências para o cumprimento de missões nos níveis estratégico, operacional ou tático. Para tanto, na composição dessa estrutura, estão presentes elementos de ligação interagências e elementos civis especialistas (BRASIL, 2017b, p. 5-4).

No SMDC, as ações no espaço cibernético devem estar contextualizadas nos níveis de decisão político, estratégico, operacional e tático, como consta na FIG. 1 do (ANEXO).

Conforme apresentado na FIG. 2 do ANEXO, o nível de decisão político compreende as ações de Segurança da Informação e Comunicações (SIC) e Segurança Cibernética, abrangendo a Administração Pública Federal (APF) e as infraestruturas críticas da informação inerentes às infraestruturas críticas nacionais; e tem como principais atores o

---

3 Infraestruturas críticas — instalações, serviços, bens e sistemas que, se tiverem seu desempenho degradado, ou se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade.

4 O Sistema Militar de Comando e Controle (SISMC) — do Ministério da Defesa (MD), objetiva otimizar o exercício da direção, do controle e da coordenação das forças militares em operação, possibilitando o acompanhamento em tempo real das ações em curso.

Presidente da República e o Comitê Gestor da Internet no Brasil (CGI.br) (BRASIL, 2014, p. 17 e 25). Esse nível estabelece os objetivos políticos do planejamento, preparo e emprego conjunto das FA; orienta e conduz o processo global da conquista ou da manutenção desses objetivos; e decide sobre o emprego das Forças (BRASIL, 2011, p. 21).

O nível de decisão estratégico, ilustrado na FIG. 2 do ANEXO, compreende as ações de Defesa Cibernética, que ficam a cargo do MD e do EMCFA, por intermédio do ComDCiber, bem como dos Comandos das FA, por meio de seus respectivos órgãos de Defesa Cibernética (BRASIL, 2014, p. 25). Esse nível possui como fundamento para os planejamentos estratégicos os documentos de mais alto nível do País, como a Constituição Federal, as Leis Complementares que tratam da organização, do preparo e do emprego das FA, a Política de Defesa Nacional (PDN) e a END.

O nível de decisão operacional, ilustrado na FIG. 2 do ANEXO, fica a cargo dos Comandos Operacionais e de seus Estados-Maiores, quando ativados, e abrange as ações de GC. As ações de GC são aquelas que envolvem o emprego de ferramentas disponíveis no campo da TI e Comunicações para desestabilizar os ativos de informação do inimigo; e, também, para possibilitar a proteção dos ativos de interesse (BRASIL, 2014 p. 26).

Quanto ao nível de decisão tático, ilustrado na FIG. 2 do ANEXO, quando ativado, ele também abrange as ações de GC, porém, estas ficam a cargo das Forças Componentes e do Destacamento Conjunto de GC. Esse destacamento conjunto poderá ser constituído pelo ComDCiber para atuar em operações que requeiram uma coordenação em nível estratégico. O Destacamento terá, em sua estrutura, comandante e subcomandante, elementos especializados em GC das FA, elementos de ligação e civis especialistas para operação assistida e assessoria. O detalhamento da estrutura, assim como o seu efetivo, será definido e proposto após estudos, levando-se em conta as necessidades específicas de cada operação e os fatores de decisão (BRASIL, 2014, p. 30).

2.2 As Ações Cibernéticas

No contexto, de grande facilidade de acesso às informações e com a presença constante de ameaças cibernéticas, o MD define a Guerra Cibernética composta por um conjunto de ações cibernéticas que correspondem ao uso ofensivo e defensivo de Sistemas de Tecnologia da Informação e Comunicações (TIC) para defender os próprios sistemas de TIC e de Comando e Controle; ou para desestabilizar ou tirar proveito dos Sistemas de interesse (BRASIL, 2014, p. 19). Tais ações podem ser desferidas para obtenção de vantagem, tanto na área militar quanto na área civil.

As ações cibernéticas, como definido na Doutrina Militar de Defesa Cibernética, são aquelas que envolvem o emprego de ferramentas disponíveis no campo da TI e Comunicações para desestabilizar os ativos de informação do inimigo; e para possibilitar a proteção dos ativos de interesse (BRASIL, 2014, p. 23). As ações cibernéticas são de três tipos: ataque cibernético, exploração cibernética e proteção cibernética.

O ataque cibernético compreende as ações destinadas a interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais armazenados em dispositivos e redes de computadores e de comunicações do inimigo. Essa técnica emprega códigos computacionais contra alvos como servidores, *firewalls*, sensores de rede, protocolos, sistemas operacionais e *hardwares* de computadores, ou, até mesmo, contra o sistema de armas do oponente. O ataque cibernético pode abranger, inicialmente, ações de exploração cibernética que visem preparar o ataque, constituindo-se nos procedimentos iniciais para a consecução do ataque. Esse tipo de ação deve ser consistente com o arcabouço normativo legal e vigente (BRASIL, 2017b, p. 4-3).

A exploração cibernética consiste das ações de busca e coleta de informações dos ativos, executadas a fim de obter a consciência situacional do ambiente alvo. Essas ações devem, preferencialmente, evitar o rastreamento da exploração e servir como fonte de conhecimento; ou servir, apenas, como um meio para a identificação das vulnerabilidades do sistema de informação de interesse (BRASIL, 2014, p. 23). Da mesma forma, essa atividade de exploração, devido à sua característica de dualidade, também permite, de forma proativa, identificar antecipadamente possíveis ações hostis que possam ser deflagradas contra sistemas de informação a serem protegidos. Nessa situação, os dados gerados devem ser tempestivamente analisados e encaminhados aos responsáveis pelos ativos em risco, para que sejam realizados procedimentos de mitigação das vulnerabilidades identificadas. Do mesmo modo que o ataque cibernético, a exploração cibernética deve atender a orientação do arcabouço normativo e legal em vigor.

A proteção cibernética é uma atividade de caráter permanente, que compreende ações para neutralizar ataques e exploração cibernética do oponente contra os sistemas de redes computacionais e de comunicações a serem defendidos. A proteção cibernética tem por objetivo incrementar ações de Segurança e Defesa Cibernética, incluindo a detecção, a identificação e a resposta a ações que foram realizadas ou que estejam prestes a serem conduzidas pelo inimigo. Esta ação cibernética abarca o conceito de defesa em profundidade, o qual consiste em introduzir múltiplas camadas de proteção de forma a reduzir a

probabilidade de comprometimento dos sistemas de informação amigos, pois reduz o impacto das tentativas de ataque e exploração cibernética do oponente (BRASIL, 2017b, p. 4-3).

2.3 Estrutura do Espaço Cibernético da MB

A Estrutura do Espaço Cibernético da MB (ECIBER-MB) é aderente à orientação do SMDC, do MD, com suas Organizações Militares (OM) tendo atribuições e responsabilidades que permeiam os níveis de decisão estratégico, operacional e tático. A estrutura do ECIBER-MB é representada na estrutura organizacional da TI da MB, e tem, no seu nível estratégico, o Estado-Maior da Armada (EMA), o Conselho de TI da Marinha (COTIM), a Comissão Técnica de Tecnologia da Informação (COTEC-TI) e a Diretoria-Geral do Material da Marinha (DGMM) (BRASIL, 2007).

O COTIM é um órgão consultivo, deliberativo e de caráter permanente, tendo o propósito de assessorar o Comandante da Marinha, dentro da estrutura de TI da MB, no trato dos assuntos de alto nível, relacionados à Governança de TI na MB. Já a COTEC-TI é o órgão técnico de assessoria do COTIM que realiza estudos e delibera sobre os assuntos de TI e Defesa Cibernética na MB, junto ao COTIM. A DGMM supervisiona a execução das deliberações do COTIM que são implementadas pela Diretoria de Comunicações e Tecnologia da Informação da Marinha (DCTIM) (BRASIL, 2007, p. 3-2).

Permeando os níveis estratégico e operacional, com atividades presentes nos dois níveis, atua a DCTIM, como órgão de Diretoria Especializada (DE), tendo a finalidade de assegurar, permanentemente, a segurança e a defesa cibernética do ECIBER-MB no âmbito administrativo da MB (BRASIL, 2007).

Nos níveis operacional e tático, atua o Centro de Tecnologia da Informação da Marinha (CTIM), órgão de execução operacional diretamente subordinado à DCTIM. Nesses níveis, compete ao CTIM assegurar a SIC, bem como garantir a proteção cibernética na Rede de Comunicações Integradas da Marinha (RECIM) (BRASIL, 2007).

No nível tático, atuam os Centros Locais de Tecnologia da Informação (CLTI) como elementos organizacionais de apoio ao CTIM, com várias atribuições, dentre as quais, cabe ressaltar: o apoio ao CTIM na resolução dos problemas relacionados à TI; o tratamento e resposta a incidentes de SIC; a implementação de procedimentos que auxiliem na garantia da SIC dos ativos de informação da RECIM e a na garantia, manutenção e disponibilidade, em primeiro escalão, dos recursos de telecomunicações da MB, da infraestrutura da RECIM e da infraestrutura do Centro de Dados local, que atendam às OM sob sua jurisdição (BRASIL, 2007).

2.4 Infraestruturas Críticas

A partir do estabelecimento do setor cibernético, decorrente da aprovação da END, dois campos passaram a ser reconhecidos: a Segurança Cibernética, cuja responsabilidade é da Presidência da República; e a Defesa Cibernética, que fica a cargo do MD, por meio das FA. Cabe ressaltar que, no contexto do MD, no nível de decisão político, destacam-se as necessidades de se buscar a Segurança da Informação e a Segurança Cibernética, além, da necessidade de proteção das infraestruturas críticas da informação nacionais (BRASIL, 2014, p. 17).

As infraestruturas críticas de um país são aquelas que promovem o funcionamento dos serviços essenciais que afetam diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade. Normalmente, essas infraestruturas são representadas por instalações, serviços, bens e sistemas que, se tiverem seu desempenho degradado, ou se forem interrompidos ou destruídos, provocam grande impacto à segurança do Estado e da sociedade (BRASIL, 2014, p. 19).

No âmbito da MB, podem ser consideradas infraestruturas críticas: sistemas de comando e controle, bases navais, estações rádio, meios navais e sistemas diversos, tais como os de logística e abastecimento, Centros de Desenvolvimento e de Tecnologia, enlaces satelitais, redes locais de alta sensibilidade e a RECIM; ou seja, as infraestruturas que constituem o subconjunto dos ativos de informação que afetam diretamente a consecução e a continuidade da missão da MB e a segurança do seu pessoal (BRASIL, 2019b, p. 7-3).

Nesse contexto, de necessidade permanente de proteção das infraestruturas críticas nacionais, as Forças Armadas devem estar aderentes a este fundamento e preparadas para envidar esforços na execução de procedimentos que promovam o fortalecimento da defesa cibernética, com o objetivo de assegurar a proteção regular de suas infraestruturas de informações críticas.

3 EXERCÍCIOS NO ESPAÇO CIBERNÉTICO — ECIBER

A revolução tecnológica elevou o espaço cibernético a uma nova condição nos assuntos relacionados à defesa e segurança; e, atualmente, este espaço é considerado um dos cinco domínios operacionais que permeiam os outros domínios, já conhecidos, que são: o terrestre, o marítimo, o aéreo e o espacial, sendo todos interdependentes.

As atividades no espaço cibernético criam liberdade de ação para as atividades nos outros domínios, da mesma forma, atividades dos outros domínios podem criar efeitos dentro ou através do espaço cibernético (BRASIL, 2014, p. 18).

No espaço cibernético, são realizadas as atividades de Defesa e/ou de Guerra Cibernética, sendo a primeira composta por ações que são planejadas e implementadas no nível de decisão estratégico; e a segunda, composta por ações a serem empregadas no nível de decisão operacional ou tático.

Hoje, dentre o universo de informações que trafegam neste novo domínio, podem ser encontradas informações sobre aeronaves, embarcações, bases locais de apoio, centros estratégicos de controle, sistemas de apoio à decisão, dentre diversas outras informações com elevado grau de importância para um Estado, e sem limites geográficos que dificultem, minimamente, a obtenção destas informações.

As ações de guerra cibernética, hoje, são consideradas Ações de Guerra no espaço cibernético; podendo ser enquadradas quanto ao nível de emprego, tipo, efeito desejado e contexto de emprego (BRASIL, 2017a, p. 25).

Os clássicos princípios de guerra se aplicam a todos os tipos de operações militares, incluindo as ações cibernéticas. Contudo, as características e particularidades da guerra cibernética impõem que outros novos princípios sejam considerados, tais como: do efeito, da dissimulação, da rastreabilidade e da adaptabilidade, os quais serão detalhados a seguir.

Dessa forma, os princípios de emprego da guerra cibernética são: o princípio do efeito, onde as ações devem se traduzir em vantagens estratégica, operacional ou tática; o princípio da dissimulação, onde o objetivo é dificultar a rastreabilidade das ações executadas; o princípio da rastreabilidade, onde são adotadas medidas para se detectar ações ofensivas e exploratórias; e o princípio da adaptabilidade, em que se busca a capacidade de adaptação da Guerra às características de mutabilidade do espaço cibernético, que podem ser súbitas e imprevisíveis (BRASIL, 2017b, p. 2-3).

Contendo esses princípios de guerra, as ações cibernéticas podem estar presentes em qualquer operação militar, possibilitando abarcar experiência, novos conhecimentos e oportunidade de se criar novos princípios para esta dimensão ainda tão nova e mutante que é a do espaço cibernético.

Nesse sentido, além das operações militares, faz-se também necessária a presença das ações cibernéticas na prática de exercícios militares que permitam o conhecimento, o treinamento, o preparo e o desenvolvimento de novas capacidades para enfrentar possíveis

conflitos que possam ocorrer, normalmente de forma silenciosa, neste moderno campo de batalha.

De acordo com o previsto pelo MD, o planejamento e o emprego das FA Nacionais se materializam na realização de operações e exercícios de treinamento conjuntos, com os atores envolvidos atuando de forma integrada. Nas operações, põe-se em prática a experiência adquirida; já por meio dos exercícios, é possível avaliar e aprimorar a capacidade de resposta a situações adversas (BRASIL, 201-?).

Dessa forma, atualmente, os exercícios no espaço cibernético já são uma realidade necessária e prática constante em vários Estados. Sejam os de caráter militar, coordenados no âmbito da Defesa, ou de caráter privado, restritos aos órgãos do setor privado, público ou internacional, todos são realizados de forma coordenada, podendo integrar representantes de diferentes organizações e/ou países.

3.1 A identificação dos Exercícios Cibernéticos na Literatura

Com a tecnologia de sistemas de informação evoluindo mais rapidamente que as tecnologias de segurança voltada para esses sistemas, o desconhecimento sobre novas ameaças e seus riscos e o aumento da dependência do setor privado por sistemas de Tecnologia interconectados, grandes potências como os Estados Unidos, a China e a Rússia já há algum tempo investem fortemente em unidades de GC (CLARKE, 2015, p. 86 e 87).

Contudo, não basta apenas investir nas ações ofensivas de guerra cibernética. Uma medida realística de força na guerra cibernética também inclui dois fatores: a defesa e a dependência. Defesa é a medida da habilidade de um Estado em tomar ações diante de um ataque, sendo que estas ações bloquearão ou mitigarão o ataque. Já a dependência é a extensão da conectividade de um Estado e o grau de confiança que é depositado em redes e sistemas que podem se tornar vulneráveis em caso de ataque cibernético. Como exemplo de dependência cibernética, podem ser citadas as infraestruturas críticas que são dependentes de sistemas em rede e não possuem um *backup* real (CLARKE, 2015, p. 122).

Para um Estado sobreviver a uma guerra cibernética, com baixos custos, é relevante que sejam exercitadas habilidades nas ações ofensivas e defensivas, assim como medidas devem ser testadas para que, em determinadas situações, seja reduzida a dependência cibernética de setores críticos (CLARKE, 2015, p. 122).

Duas medidas importantes são identificas por Clarke em seu livro *Guerra Cibernética*, a serem implementadas como forma de incrementar as habilidades descritas acima e, consequentemente, elevar a capacidade cibernética. A primeira medida trata da

necessidade de o Estado regulamentar, por meio de uma Estratégia (norma), diversos objetivos e ações e, dentre estes, a necessidade relevante de o Estado se preocupar com as infraestruturas críticas operadas pela iniciativa privada, e não estar voltado somente para os sistemas ou infraestruturas do Governo.

A segunda, trata da importância da realização de Exercícios Cibernéticos. Há uma razão pela qual os militares realizam repetidos exercícios de treinamento simulados: para garantir que as FA sejam capazes de responder a ataques militares de maneira imediata e eficaz.

Não é de admirar que governos de todo o mundo tenham feito o mesmo, no que diz respeito ao ECIBER. Curiosamente, enquanto a ameaça de invasão física de qualquer país ocidental diminui a cada ano, a ameaça de ataques cibernéticos aumenta drasticamente. Um ataque cibernético tem o potencial de dizimar os sistemas vitais de muitos países, incluindo transporte e infraestrutura (energia, água, bancos e assistência médica). Desse modo, os Exercícios Cibernéticos ajudam os governos a planejar ataques, aumentar a segurança e diminuir a chance de sucesso dos ataques do oponente que poderiam provocar resultados altamente comprometedores.

Um dos primeiros exercícios cibernéticos de treinamento tático e simulado — entenda-se por virtual — foi chamado de *Cyber Storm*. Este exercício ocorre desde 2006 e permite ao Departamento de Segurança Interna dos Estados Unidos se preparar para ataques, destacando vulnerabilidades, não somente em sistemas eletrônicos, mas também em sua resposta a um ataque (CLARKE, 2015, p. 146).

Em sua primeira edição, ocorrida em 2006, um dos principais objetivos era verificar o tempo de preparação e resposta de diferentes sistemas e departamentos para um ataque em todas as frentes, incluindo suas infraestruturas críticas. O ataque controlado e simulado foi alavancado contra alvos importantes, incluindo, como exemplo, o sistema de transporte de metrô de Washington DC, instalações críticas na Filadélfia, Chicago e interrupção de serviços públicos em Los Angeles (SHEVES, 2017).

O resultado do exercício revelou a incapacidade de sistemas e departamentos de identificar ataques com rapidez suficiente e não conseguir se concentrar na totalidade dos ataques, mas em incidências específicas. No geral, verificou-se que, se estivessem sob ataque real, não seriam capazes de se defender e responder, adequadamente, com a agilidade necessária.

Outro exercício cibernético, que ocorre desde 2005, é o *Silent Horizon* (CLARKE, 2015, p. 146). Este exercício, administrado pelo Centro de Operações de Informação da

Agência Central de Inteligência (CIA), simula a guerra cibernética. Nele, em sua primeira edição, simulou-se um cenário de cinco anos no futuro, em que um ataque na mesma proporção dos ataques de 11 de setembro ocorreria e incluiria *hackers* contratados por organizações antiamericanas. Na ocasião, buscou-se demonstrar que o impacto dos ataques cibernéticos poderia ter proporções tão relevantes quanto as dos ataques de 11 de setembro, causados por terroristas, contrariando a crença de especialistas dos EUA de que efeitos tão abrangentes seriam improváveis. Este exercício contou com a participação de cerca de 75 representantes, principalmente da CIA, respondendo a diferentes tipos de ataques.

O *Locked Shields* é outro exercício que ocorre anualmente. Ele é considerado um exercício de Defesa Cibernética do tipo *live-fire*, ou seja, que envolve desafios para equipes azul e vermelho; ele é organizado pelo *Cooperative Cyber Defense Centre of Excellence* (CCDCOE) da Organização do Tratado do Atlântico Norte (OTAN), desde 2010. O exercício permite que os especialistas em segurança cibernética aprimorem suas habilidades na defesa dos sistemas nacionais de TI e de infraestrutura crítica sob ataques simulados em tempo real.

O objetivo desse exercício é fornecer cenários cibernéticos realistas, e não apenas atividades do tipo *Capture The Flag* (CTF); assim como o treinamento das equipes de resposta a incidentes e das equipes de ataque e de defesa. Nele, são utilizadas tecnologias de ponta e simulação de toda complexidade de um incidente, abordando aspectos estratégicos de decisão, aspectos jurídicos e de comunicação.

Na edição do *Locked Shields*, ocorrida em 2019, mais de 1.200 especialistas de quase 30 países participaram do exercício, no qual a equipe francesa emergiu como a vencedora. O exercício foi organizado pelo CCDCOE, em cooperação com as Forças de Defesa da Estônia, as Forças de Defesa da Finlândia, o Comando Europeu dos Estados Unidos, o Instituto Nacional de Pesquisa de Segurança da República da Coreia e a Universidade de Tecnologia de Tallinn, Estônia (CCDCOE, 2019).

Outro exercício cibernético também de grande relevância é o realizado pelo Exército Português, conhecido como *Cyber Perseu*. Este exercício nacional de defesa cibernética é planejado e conduzido pelo Exército Português desde 2014, com o objetivo de testar e avaliar a capacidade de detecção, resposta e coordenação com as principais entidades governamentais e privadas daquele país perante ataques cibernéticos em grande escala. Na sua edição de 2017, participaram mais de 60 empresas privadas e representantes de universidades, órgãos do Estado e do Exército.

Na edição de 2017, foram implementados procedimentos que permitiram coordenar melhor as respostas perante incidentes cibernéticos; e, de forma complementar, o

Exército Português realizou competições de CTF, com o propósito de penetrar e atingir objetivos dentro de infraestruturas simuladas, as quais lhes permitiram identificar os especialistas com mais conhecimentos e habilidades.

Nas recentes edições do *Cyber Perseu*, o Exército Português vem possibilitando o acesso e a participação na estrutura do exercício de um conjunto diversificado de entidades nacionais militares e civis, do setor público e privado, de nações aliadas e amigas, que aproveitam a ocasião para conduzir o seu próprio treino e exercitar a habilidade de integração junto aos demais participantes do exercício (CORREIA, 2019).

Clarke (2015, p. 146) recomenda em seu livro: "não lute contra o enredo", ou seja, não se deve rejeitar a premissa de que, em algum dia, algum Estado possa estar à beira de um conflito cibernético. Diante disso, ao entendermos os riscos e a nossa postura atual em relação a uma guerra cibernética simulada, podemos reduzir as chances de sermos derrotados em uma guerra cibernética real. E, caso ela aconteça, é melhor ter pensado, antecipadamente, como ela pode ser.

Dessa forma, conclui-se que, ao longo dos anos, desde o despertar para o espaço cibernético como mais um domínio de guerra, muitos países, como os aqui citados, já realizam exercícios cibernéticos periodicamente, agregando conhecimentos e experiências em cada edição realizada.

3.2 Exercício Cibernético no âmbito do MD

No âmbito do MD, o ComDCiber, atendendo à Diretriz Ministerial nº 14 do MD (BRASIL, 2009), a END e a Estratégia Nacional de Segurança Cibernética, coordena e integra ações referentes ao setor estratégico Cibernético, tais como: o planejamento, a orientação e a execução das atividades relacionadas ao desenvolvimento e aplicação das capacidades cibernéticas. Atuando como órgão central do SMDC, o ComDCiber contribui para o uso efetivo do espaço cibernético, impedindo ou dificultando sua utilização contra os interesses da Defesa Nacional.

O ComDCiber, desde 2018, realiza o exercício cibernético chamado "Guardião Cibernético", atualmente o único exercício cibernético no âmbito nacional. Esse exercício tem o objetivo de desenvolver a coordenação e integração entre setores da Segurança e Defesa Cibernética, envolvendo áreas do Governo, Defesa, academia e setor privado, com interesses e responsabilidades correlatas, e de buscar a elevação do nível de proteção das infraestruturas críticas nacionais, assim como o nível de maturidade da sociedade em segurança cibernética.

O exercício Guardião Cibernético está alinhado com a Política Nacional de Segurança da Informação (PNSI) e com a Estratégia Nacional de Segurança Cibernética (E-Ciber) do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), as quais preconizam a elevação da proteção cibernética no âmbito do governo e das infraestruturas críticas, por meio de ações baseadas na cooperação e integração. A segunda edição do exercício, ocorrida em 2019, teve por finalidade contribuir para o incremento do nível de proteção do ECIBER nas infraestruturas críticas em seus setores elétrico, financeiro, nuclear e de telecomunicações (SILVA, 2019).

Além dos representantes dos setores das infraestruturas críticas citadas, também houve a participação de representantes de órgãos parceiros, da comunidade acadêmica e de observadores internacionais do CCDCOE da OTAN e de nações amigas, como os Estados Unidos da América, Portugal, Suécia e Tailândia.

O ComDCiber, nesta edição de 2019, traçou alguns objetivos para serem alcançados, dentre os quais, podem ser destacados: o exercício do processo de decisão em diferentes níveis de responsabilidade e competência; a verificação da efetividade dos procedimentos executados para a solução dos possíveis incidentes que venham afetar as infraestruturas críticas; a aplicação de boas práticas de proteção cibernética nas ações de prevenção e reação mediante os incidentes simulados ocorridos; utilização de ferramentas para o compartilhamento de informações; e a possibilidade de que as empresas e organizações participantes treinem procedimentos, com a finalidade de aprimorar seus processos internos (SILVA, 2019).

O exercício utilizou técnicas de simulação virtual e construtiva. Onde a primeira identifica e difunde as melhores práticas de tratamento e resposta a incidentes de rede. Enquanto a segunda, permite exercitar o nível gerencial das organizações na identificação e solução de problemas, envolvendo as áreas de SIC, departamento jurídico e comunicação social (SILVA, 2019).

Foi empregado neste exercício um cenário cibernético fictício, envolvendo as FA e as áreas estratégicas de interesse para a Defesa Nacional, buscando-se a criação de incidentes úteis para a verificação de processos e protocolos, visando à obtenção de ensinamentos para a melhoria e elevação do nível de proteção cibernética.

O artigo menciona que na terceira edição do exercício Guardião Cibernético, prevista para o ano de 2020[5], o exercício contaria com algumas evoluções, tais como: a inserção dos setores de Água e de Transporte Aéreo; e a introdução de desafios da próxima década, envolvendo algumas tecnologias, como a inteligência artificial, as redes de cabos submarinos e a telefonia móvel 5G (SILVA, 2019).

Dessa forma, o ComDCiber, no âmbito do MD, com a realização do exercício Guardião Cibernético, contribui para o incremento do conhecimento e da experiência e o fortalecimento da necessária resiliência cibernética. Com o exercício, busca-se a proteção não somente dos sistemas de interesse do governo, mas também a dos sistemas dos órgãos representantes das infraestruturas críticas do País, uma vez que é reconhecida a necessidade de se evitar os riscos de comprometimento destas infraestruturas, pois estes causariam sérios impactos no âmbito social, econômico, político e internacional, afetando, consequentemente, a soberania e a Defesa Nacional.

Conforme exposto, observa-se que, por meio do exercício cibernético nacional, é possível obter-se a coordenação e integração entre os níveis de decisão político e estratégico, inseridos no SMDC, atendendo ao preconizado nas normas nacionais, buscando exercitar, na prática, tanto os procedimentos afetos à segurança cibernética das infraestruturas críticas no nível político, quanto os procedimentos afetos à defesa cibernética no nível estratégico.

4 CONTRIBUIÇÕES PARA A SEGURANÇA E DEFESA CIBERNÉTICA

Com a natureza complexa e difusa do espaço cibernético, provavelmente as organizações estejam correndo o risco de sofrer ataques semelhantes, o que ressalta a importância do compartilhamento de informações sobre o ataque, do tratamento a ser dado a ele, bem como das lições aprendidas. Nesse contexto, visando à segurança e à defesa cibernéticas, considera-se de grande relevância o estabelecimento de um ambiente de resposta coordenado e cooperativo, que ganhe eficácia com a interoperabilidade entre os setores público, privado, acadêmico e a sociedade.

5 Esta terceira edição do exercício Guardião Cibernético, que estava prevista para o ano de 2020, foi cancelada devido à pandemia mundial da COVID-19.

4.1 Identificação das contribuições resultantes da realização dos Exercícios Cibernéticos

Após a apresentação dos exercícios cibernéticos, algumas contribuições para a segurança e defesa cibernética podem ser destacadas. Segue o detalhamento das principais contribuições observadas, tais como: a capacitação e o aprimoramento dos processos de tomada de decisão; o aprimoramento da capacidade de resposta e tratamento a incidentes de segurança; o aprimoramento do arcabouço normativo; o fortalecimento da proteção das infraestruturas críticas; e o fomento à cooperação e integração nacional e internacional.

4.1.1 A capacitação e o aprimoramento dos processos de tomada de decisão

O investimento no fator humano por meio do treinamento individual ou coletivo é fundamental. Exercícios como o *Cyber Storm*, o *Silent Horizon*, o *Locked-shields*, *Ciber Perseu* e o "Guardião Cibernético" permitem testar capacidades em ambientes controlados e identificar lacunas em procedimentos, ferramentas e capacitação; assim como estabelecer relações de confiança entre os participantes, necessárias à coordenação e cooperação entre os membros da comunidade cibernética.

A possibilidade de se identificar pessoas com habilidades e capacidades cibernéticas é uma contribuição relevante, uma vez que o conhecimento na área é muito específico. Além disso, os exercícios proporcionam, aos participantes, o conhecimento e a manipulação de novas técnicas e ferramentas, por consequência da integração entre os diversos atores envolvidos.

Normalmente, os gestores de Tecnologia da Informação (TI) não estão totalmente cientes das implicações que podem resultar dos produtos e soluções de tecnologia relacionados à segurança, assim como os técnicos em TI não são familiarizados com os processos de tomada de decisões. Dessa forma, os exercícios providenciam a oportunidade do treinamento para ambos os segmentos profissionais, além de uma maior proximidade entre estes atores.

Nesse sentido, em exercícios como o *Ciber Perseu* e o "Guardião Cibernético", por exemplo, são construídas simulações construtivas, que permitem aos participantes praticar as decisões gerenciais na solução de problemas em suas organizações, envolvendo, também, a área jurídica e de comunicação social (SILVA, 2019).

4.1.2 O aprimoramento da capacidade de resposta e tratamento a incidentes de segurança

Outra entrega igualmente importante dos exercícios ocorre por meio da simulação virtual de ambientes reais, com inúmeros desafios, que tem por objetivo identificar e difundir

melhores práticas para as equipes de resposta e tratamento de incidentes das organizações, assim como difundir a importância do compartilhamento de informações entre estas equipes (SILVA, 2019).

As equipes de resposta e tratamentos a incidentes são elementos sempre presentes nos exercícios cibernéticos. Essas equipes estão presentes em grande parte das organizações públicas ou privadas. Normalmente, encontram-se inseridas em Centros, conhecidos pela sigla CSIRT, que significa *Computer Security Incident Response Team*. As equipes devem estar capacitadas para identificar, analisar, tratar e responder a notificações sobre incidentes de segurança dentro das organizações, podendo exercer funções reativas ou proativas, para auxiliar na proteção dos recursos críticos (BRASIL,2020).

Durante os exercícios, são treinadas as habilidades reativas e proativas destas equipes, abrangendo o incremento da conscientização, detecção de intrusões, testes de penetração, elaboração de documentação e, até mesmo, o registro da necessidade de desenvolvimento de programas específicos. Tais habilidades, treinadas durante os exercícios, colaboram para que a organização exercite a prevenção aos incidentes de segurança, bem como aprenda a importância de diminuir o tempo de resposta quando um incidente ocorrer.

Outro ganho positivo para as equipes de CSIRT e para todas as organizações participantes é o compartilhamento de informações e estratégias de respostas que ocorrem por meio do incentivo ao relacionamento entre diversos CSIRTs e organizações durante o exercício. Cabe ressaltar que, segundo a E-Ciber, o compartilhamento de informações é uma forma de evidenciar a parceria estratégica entre as entidades interessadas em segurança cibernética.

4.1.3 O aprimoramento do arcabouço normativo

Durante a segunda edição do exercício Guardião Cibernético, aproveitou-se o cenário integrado do exercício para implementar, a título de teste, a minuta do Plano Nacional de Tratamento de Incidentes de Redes, com o objetivo de registrar impressões e colher subsídios para, posteriormente, encaminhá-los para validação por parte do GSI/PR (SILVA, 2019).

Assim, observa-se a contribuição que também pode ocorrer na dimensão normativa. Devido à característica evolutiva do tema cibernético, há a necessidade do acompanhamento das mudanças e constante atualização do arcabouço normativo. Com os exercícios, há a oportunidade de que os atores envolvidos possam aproveitar a dinâmica dos vários cenários proporcionados para colher experiências e criar ou reavaliar os seus

instrumentos normativos e procedimentos. Cabe ressaltar que a E-Ciber prevê que sejam realizadas ações que contribuam para o aprimoramento do arcabouço normativo sobre segurança cibernética, por acreditar que tais iniciativas auxiliam no necessário alinhamento estratégico e normativo, fundamentais nesta área.

4.1.4 O fortalecimento da proteção das infraestruturas críticas

A proteção das infraestruturas críticas — estas normalmente representadas pelos setores de Telecomunicações, Energia, Transportes, Água e Financeiro — são o escopo das Estratégias (normas) de alguns países e principal foco dos exercícios elencados neste trabalho. Algumas Estratégias nacionais destacam que ataques às infraestruturas críticas representam as maiores ameaças à segurança e defesa nacional.

Dessa forma, durante os exercícios, busca-se realizar simulações nestes setores, para que as equipes de CSIRT possam: identificar os níveis adequados de segurança e de resiliência a serem alcançados; os meios para se garantir a continuidade da prestação dos serviços; o fortalecimento da integração e cooperação de diferentes atores dos setores público e privado, do âmbito nacional e internacional; bem como, identificar e conhecer as possíveis formas de mitigar os mais variados tipos de ataques que possam ser direcionados a essas estruturas (SILVA, 2019).

4.1.5 O fomento à cooperação e integração nacional e internacional

Outra contribuição fundamental dos exercícios, e igualmente prevista em Estratégias de alguns Estados, é a necessidade da obtenção e manutenção da cooperação e integração envolvendo o governo, academia, o setor privado e a defesa, aliados à cooperação e interação internacional. Em meio às ameaças que evoluem continuamente no espaço cibernético, a busca por parcerias estratégicas é um caminho relevante para a troca de informações e garantia de unidade de esforços.

Como ensinamentos colhidos dos exercícios, fruto do ambiente colaborativo fomentado, pode-se elencar a constante troca de experiências afetas às boas práticas executadas pelos elementos participantes e o conhecimento mútuo sobre as possibilidades e limitações dos diversos setores nacionais e países participantes que integram o espaço cibernético.

Um exemplo de fruto colhido da integração e cooperação entre países, é a parceria estratégica estabelecida entre o ComDCiber e o Centro de Defesa Cibernética de Portugal. Esta parceria está possibilitando, ao setor da Defesa, o teste de uma plataforma de

compartilhamento de informações on-line sobre artefatos maliciosos. Essa plataforma, atualmente, é amplamente utilizada pelos países integrantes da OTAN (SILVA, 2019).

Foi possível observar que o exercício Guardião Cibernético, conduzido pelo ComDCiber, buscou um estreito alinhamento com a mais recente norma sobre a Estratégia Nacional de Segurança Cibernética, onde o exercício contribuiu para o alcance de algumas Ações Estratégicas (AE), contempladas nos eixos temáticos da referida norma, tais como: promover ambiente participativo, colaborativo, confiável e seguro, entre o setor público, setor privado e sociedade (AE3); elevar o nível de proteção das Infraestruturas Críticas Nacionais (AE5); aprimorar o arcabouço legal sobre segurança cibernética (AE6); ampliar a cooperação internacional do Brasil em segurança cibernética (AE8); ampliar a parceria, em segurança cibernética, entre setor público, setor privado, academia e sociedade (AE9); e elevar o nível de maturidade da sociedade em segurança cibernética (AE10) (BRASIL,2020).

O espaço cibernético não conhece fronteiras. Assim, percebe-se que os exercícios cibernéticos, de âmbito nacional ou internacional, é uma oportunidade para identificar fragilidades, necessidades de investimentos e melhorias em várias áreas de atuação do governo e do setor privado. Os exercícios contribuem para o fortalecimento da cooperação e integração e para a melhoria dos processos que irão garantir a proteção das infraestruturas críticas de interesse, permitindo o ganho de experiência e habilidade na coordenação da integração entre entidades públicas e privadas, bem como angariar lições aprendidas que terão impacto na avaliação e no aperfeiçoamento do arcabouço doutrinário sobre segurança e defesa cibernética.

4.2 Os Desafios a serem superados no âmbito nacional

A E-Ciber prevê Ações Estratégicas que contribuam para o reforço das capacidades nacionais em segurança e defesa cibernética. Contudo, tanto para a Defesa, no nível estratégico, quanto para a Segurança, no político, para alcançarem a plena capacidade cibernética, alguns desafios necessitam ser identificados e superados.

A segurança e a defesa do espaço cibernético dependem, fundamentalmente, da cultura dos indivíduos em segurança. Devido à maior facilidade de acesso à Internet, com seu índice de utilização pelas empresas chegando a 98%, maior é a necessidade de se ter maturidade para o uso deste ambiente. Segundo levantamento realizado em 2019 pela Agência Senado, o Brasil ocupa a 70ª colocação no índice de segurança cibernética da União Internacional de Telecomunicações (ITU, na sigla em inglês), órgão da Organização das

Nações Unidas (ONU). Esta situação de fragilidade tornou o país o segundo alvo, no mundo, em ataques cibernéticos (BRASIL, 2019a).

Nesse contexto, destacam-se alguns desafios a serem superados, como na área de educação, nas respostas aos incidentes, na proteção das infraestruturas críticas e no âmbito da cooperação e integração nacional e internacional.

4.2.1 Educação

O primeiro desafio está na alfabetização digital da sociedade. Durante a execução dos exercícios cibernéticos citados, um dos objetivos a serem alcançados foi o treinamento, a troca de experiências em boas práticas e a obtenção de conhecimento. Contudo, ainda há que se melhorar a cultura em segurança cibernética, conforme prevê a E-Ciber.

O desenvolvimento da cultura ocorre por meio do investimento em educação, atingindo toda a sociedade, em todos os níveis de ensino, com a finalidade de reduzir a exposição aos riscos cibernéticos e incrementar a conscientização do uso responsável das tecnologias disponíveis (BRASIL, 2020).

O incentivo à educação e à alfabetização digital é um desafio a ser superado em médio a longo prazo e pode ser alcançado por meio da atuação em três frentes: Capacitação, Formação e Conscientização (BRASIL, 2020).

A capacitação compreende a educação de profissionais atuantes na área, ela representa um conhecimento mais especializado, que pode ser obtido, por exemplo, por meio de treinamentos e certificações. Nesse sentido, são necessárias ações para proporcionar mais oportunidades de treinamento aos profissionais de TI e da área cibernética, a fim de contribuir com os conhecimentos necessários às implantações das diversas tecnologias e soluções digitais.

A formação consiste em inserir a educação em segurança cibernética na educação infantil, ensino fundamental, ensino médio e superior, pois a sua abordagem ainda é incipiente nas escolas brasileiras. Nesse sentido, a E-Ciber recomenda o estabelecimento de parcerias das organizações com o Ministério da Educação, visando à implementação de programas de incentivo ao desenvolvimento de capacidades em segurança cibernética.

Já a conscientização pode ser obtida por meio de ações que sensibilizem a sociedade, alcançando usuários individuais e corporativos, inclusive crianças em seu ambiente escolar. A conscientização deve ser alcançada, de forma contínua, por meio de palestras, seminários, campanhas educativas, dentre outras ferramentas, induzindo a mudança para um comportamento favorável e seguro no uso de tecnologias disponíveis.

4.2.2 Resposta aos incidentes e proteção das infraestruturas críticas

O segundo desafio, igualmente colaborador da cultura cibernética, é a necessidade de maior agilidade nas respostas aos incidentes, o acompanhamento contínuo das ameaças e dos tipos de ataques cibernéticos, além do estabelecimento de canais de comunicação adequados com equipes internas e externas às organizações e com as entidades internacionais (BRASIL, 2020).

Em relação à proteção das infraestruturas críticas, o desafio consiste em realizar investimentos dentro de uma abordagem ampla sobre os procedimentos de segurança. Tais procedimentos colaboram significativamente com o incremento do nível de proteção das infraestruturas críticas de interesse para a Segurança e Defesa Nacional.

Dentre os procedimentos citados na E-Ciber, alguns são aqui destacados: necessidade da realização de análise de riscos; definições normativas; aumento da articulação entre os representantes das infraestruturas críticas; incentivo destas organizações à criação de uma cultura e mentalidade de segurança cibernética; criação de estrutura de governança cibernética dentro das organizações, estabelecendo procedimentos para resposta e tratamento de incidentes, controles de segurança aplicável a todos os usuários, inclusive aos terceiros, a capacitação contínua para todos os níveis e o alinhamento da segurança com os padrões nacionais e internacionais, dentre outros (BRASIL, 2020).

A resposta a incidentes cibernéticos transnacionais de larga escala requer uma fortalecida cooperação nacional e internacional, em todos os níveis de decisão, seja no nível político, estratégico ou operacional. Observa-se, também, que a cooperação e a articulação entre as redes de contato dos CSIRT nacional e internacional necessitam ser estabelecidas (BRASIL, 2020).

4.2.3 Cooperação e Integração

A preocupação com a segurança e a defesa cibernéticas é global, sendo fundamentais, portanto, a interação e a cooperação entre os diversos atores da comunidade nacional e internacional para a construção de um ambiente cibernético resiliente e confiável. Dessa forma, o desafio que está posto para o País é adotar diretrizes que, por meio de sólidas relações de confiança e de acordos estabelecidos, visem à cooperação e ao intercâmbio intenso de informações, de modo que a solução destes desafios contribua para a identificação, o gerenciamento e a mitigação dos riscos cibernéticos (BRASIL, 2020).

A cooperação e a integração facilitam o compartilhamento de informações relevantes, tais como avaliação de crises, conhecimento e análise de artefatos maliciosos, doutrinas, tecnologias emergentes, análise de ameaças persistentes, respostas e tratamento de incidentes, dentre outras.

O desafio de se estabelecer e consolidar parceiros estratégicos ganha relevância quando se constata que boa parte das infraestruturas críticas de interesse são de responsabilidade do setor privado, reforçando, com isso, a necessidade da busca constante pela cooperação e integração entre o Governo, a Defesa, o setor privado, o acadêmico e a sociedade, como um todo.

No domínio do espaço cibernético, o estabelecimento e a manutenção destas relações, o incremento da alfabetização digital e a preocupação com a proteção das infraestruturas críticas, são essenciais, já que o tema perpassa fronteiras físicas entre as nações.

Pelo o que foi exposto, conclui-se que os desafios apresentados requerem soluções de médio a longo prazo, onde os resultados somente poderão ser alcançados se todos agirem de forma coordenada, pois não há possibilidade de se obter êxito agindo de forma isolada no enfrentamento às adversidades impostas pelas novas tecnologias; e percebe-se que a realização de exercícios cibernéticos, com suas contribuições destacadas anteriormente, consiste em uma ferramenta que ajudará a superar alguns dos desafios aqui mencionados e ao alcance dos objetivos expostos nas ações estratégicas da E-Ciber.

4.3 Identificação das contribuições dos Exercícios Cibernéticos para a SIC na MB

Dentro da Estrutura Cibernética da MB, permeando os níveis estratégico e operacional, com atividades presentes nos dois níveis, atua a DCTIM. À esta Diretoria compete a elaboração, revisão e gerenciamento das normas para SIC da Marinha; o planejamento, coordenação e controle das atividades técnicas de SIC, supervisionando e analisando as atividades que venham a afetar os requisitos de SIC; assim como a coordenação e orientação das atividades do CTIM. Já este Centro, atuando nos níveis operacional e tático, tem como principais atividades as seguintes: o monitoramento da RECIM; a execução das atividades técnicas de segurança e defesa cibernética; assim como as atividades de resposta e tratamento a incidentes (BRASIL, 2019b).

A MB sempre buscou estar alinhada com as normas vigentes do âmbito da APF e do MD, com a finalidade de assegurar a proteção dos seus ativos de informação.

A primeira iniciativa neste sentido, atendendo às normas vigentes, foi a criação do seu arcabouço normativo, com a implementação inicial de uma Política de Segurança da Informação e Comunicações contendo diversas normas sobre SIC direcionadas ao público interno da MB. Essa política foi criada sendo aderente às orientações propostas na Instrução Normativa nº 01 GSI/PR/2008 (BRASIL, 2019b).

Com a criação das normas, instruções técnicas, boletins técnicos, procedimentos, doutrinas, dentre outros documentos e procedimentos, buscou-se garantir os requisitos de SIC, tais como a confidencialidade, a integridade, a disponibilidade e a autenticidade dos ativos de informação da MB. Atualmente, todos esses requisitos são garantidos por meio da execução de procedimentos e ferramentas, visando à confidencialidade, que consiste na garantia de que a informação não será disponibilizada ou revelada a pessoas ou sistemas não autorizados ou credenciados; a integridade, que garante que a informação não será modificada ou destruída; a disponibilidade, que garante que a informação sempre estará disponível; e a autenticidade, que consiste em identificar e registrar a pessoa ou sistema que produz, envia ou modifica uma informação (BRASIL, 2019b).

Nesse sentido, são necessários mecanismos para se garantir os requisitos básicos de SIC. Na MB, a governança cibernética representa um destes mecanismos, podendo ser alcançada de várias formas, como, por exemplo, por meio da realização de fóruns e designação de gestores de segurança da informação em cada Organização Militar (OM). Outro mecanismo relevante é o aprimoramento do arcabouço legal sobre segurança, identificando temas ausentes na legislação vigente e elaborando normas sobre tecnologias emergentes. Da mesma forma, são envidados esforços para se elevar o nível de maturidade dos usuários das OM no uso consciente dos sistemas administrativos e operativos da MB, por meio de campanhas de conscientização e da inserção do tema cibernético nas escolas militares.

Ressalta-se que, além dos mecanismos citados anteriormente, outras medidas relevantes poderiam ser especialmente agregadoras de conhecimento e experiência para o incremento da proteção da informação e das infraestruturas críticas de interesse da MB.

Nesse caso, para a MB, o planejamento e a execução de exercícios cibernéticos internos à Força ou a participação de equipes técnicas em exercícios no âmbito do MD, contribuiriam significativamente para a capacitação dos indivíduos que atuam na área cibernética. Outras contribuições relevantes consistem no fomento do estabelecimento de relações de confiança, com a finalidade de incrementar o compartilhamento de informações com as demais equipes técnicas que atuam no tratamento e resposta a incidentes no âmbito do

governo e instituições privadas; no desenvolvimento e aperfeiçoamento de habilidades para o uso de novas ferramentas e procedimentos para a análise e mitigação de vulnerabilidades; e o incentivo à cooperação e integração, atualmente prezados no âmbito do MD e previstos na E-Ciber.

Ou seja, conclui-se que todas as contribuições vislumbradas anteriormente, neste trabalho, como resultado da execução de exercícios cibernéticos, igualmente se aplicariam, num escopo mais limitado, como contribuições para a Marinha reforçar, principalmente, a proteção de suas infraestruturas críticas de interesse, com destaque para o fortalecimento da proteção das organizações responsáveis pelo setor nuclear.

5 CONCLUSÃO

Ao longo dos capítulos, identificou-se a estrutura cibernética da Defesa, descrevendo a evolução do setor cibernético nacional e a condução de alguns exercícios cibernéticos no âmbito internacional e no âmbito nacional, com a respectiva análise das contribuições destes exercícios para a segurança e defesa do espaço cibernético. Destacou-se, também, a especial atenção à proteção das infraestruturas críticas de interesse, os desafios a serem superados e as possíveis contribuições que proporcionariam os exercícios cibernéticos no âmbito da MB.

Avaliaram-se, ainda, as principais contribuições resultantes da prática de se realizar exercícios cibernéticos, cujo objetivo não se resume somente ao aperfeiçoamento de procedimentos técnicos ou unicamente da proteção de sistemas de interesse dos governos, mas, também, a oportunidade do fortalecimento das relações de confiança com os atores envolvidos, seja no âmbito nacional ou internacional; e a busca incessante pela proteção das infraestruturas críticas de interesse de cada Estado. Constata-se como sendo uma das principais contribuições a de que todos os países que executam exercícios cibernéticos estão atentos e preocupados com o imensurável dano que ataques cibernéticos podem causar, caso eles atinjam suas infraestruturas críticas de interesse.

Dessa forma, os exercícios cibernéticos se tornaram uma das principais ferramentas para se avaliarem os riscos de comprometimento deste ativo crítico; assim como direcionam os procedimentos e controles necessários a serem implementados para a redução desses riscos a níveis aceitáveis.

Outra constatação interessante é a de que os exercícios identificados e citados neste trabalho foram executados visando implementar as ações estratégicas previstas nas

normas dos seus países, que refletem a busca por atingir um nível mais maduro nas capacidades cibernéticas dos Estados.

Diante disso, observou-se que as contribuições resultantes da realização dos exercícios pesquisados podem ser aplicadas ao ECIBER da MB agregando novos conhecimentos, experiências e possibilitando o aprimoramento dos processos que irão incrementar a SIC e a Defesa Cibernética desse espaço.

Entretanto, pelas pesquisas realizadas, foi possível perceber que há muitos desafios a serem superados para se atingir o nível de capacidade cibernética ideal. Essas adversidades são de toda ordem, como, por exemplo: a necessidade de se investir continuamente na educação cibernética nos bancos escolares, em todos os níveis; a necessidade da elaboração de protocolos de cooperação para melhoria do compartilhamento de informações, em âmbito nacional e internacional; e a necessidade de se obter prioridade e recursos para maiores investimentos no setor cibernético, tão crítico e essencial para prover suporte à economia, às infraestruturas, à segurança pública e à defesa nacional.

Por fim, conclui-se que, proteger cada computador de um ataque cibernético, é impossível; mas é importante conhecermos nossas fraquezas, melhorarmos procedimentos e fortalecermos a segurança das nossas redes contra os ataques cibernéticos do oponente. Igualmente, devemos criar dificuldades para que nenhum ataque venha a comprometer a capacidade de resposta das instituições ou do Estado Brasileiro. Mesmo que a segurança e a defesa não sejam perfeitas, as redes protegidas têm maiores capacidades de resiliência e de rápida recuperação.

REFERÊNCIAS

BRASIL. **Brasil é 2º no mundo em perdas por ataques cibernéticos, aponta audiência.** Publicado em: 05/09/2019a. Agência Senado. Brasília, DF, 2019. Disponível em: https://www12.senado.leg.br/noticias/materias/2019/09/05/brasil-e-2o-no-mundo-em-perdas-por-ataques-ciberneticos-aponta-audiencia. Acesso em: 10 abr. 2020.

BRASIL. Diretoria-Geral do Material da Marinha. **DGMM-0540:** Normas de Tecnologia da Informação da Marinha. 3. rev. Rio de Janeiro: Diretoria-Geral do Material da Marinha, 2019b.

BRASIL. Estado-Maior da Armada. **EMA-305:** Doutrina Militar Naval. 1. ed. Brasília, DF: Estado-Maior da Armada, 2017a.

BRASIL. Estado-Maior da Armada. **EMA-416,** Vol. I: Doutrina de Tecnologia da Informação da Marinha. 1. rev. 1. Mod. Brasília, DF: Estado-Maior da Armada, 2007. Disponível em: http://www.ema.mb/docs/publicacoes/public.html. Acesso em: 23 jul. 2020.

BRASIL. Ministério da Defesa. **Diretriz Ministerial nº 14/2009.** 2009. Publicada em 09 de novembro de 2009. Brasília, DF, 2009. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/File/legislacao/emcfa/portarias/0014a_2009.pdf. Acesso em: 28 jul. 2020.

BRASIL. Ministério da Defesa. **Estratégia Nacional de Defesa.** Brasília, DF, 2012a. Disponível em: https://www.defesa.gov.br/estado-e-defesa/estrategia-nacional-de-defesa. Acesso em: 21 fev. 2020.

BRASIL. Ministério da Defesa. **Exercícios e Operações Militares.** Brasília, DF, [201-?]. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/exercicios-e-operacoes/copy_of_exercicios-militares. Acesso em: 22 jul. 2020.

BRASIL. Ministério da Defesa. Exército Brasileiro. Comando de Operações Terrestres. **EB70-MC-10.232:** Manual de Campanha, Guerra Cibernética. Brasília, DF, 2017b. Disponível em: http://bdex.eb.mil.br/jspui/bitstream/1/631/3/EB70MC10232.pdf. Acesso em: 23 jul. 2020.

BRASIL. Ministério da Defesa. **MD30-M-01:** Doutrina de Operações Conjuntas. 1º Vol. Brasília, DF, 2011. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/legislacao/emcfa/publicacoes/doutrina/md30a_ma_01a_volumea_1.pdf. Acesso em: 28 jul. 2020.

BRASIL. Ministério da Defesa. **MD31-M-07:** Doutrina Militar de Defesa Cibernética. Brasília, DF, 2014. Disponível em: https://www.defesa.gov.br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31_m_07_defesa_cibernetica_1_2014.pdf. Acesso em: 22 fev. 2020.

BRASIL. Ministério da Defesa. **MD31-P-02:** Política Nacional de Defesa. Brasília, DF, 2012b. Disponível em: https://www.defesa.gov.br/estado-e-defesa/politica-nacional-de-defesa. Acesso em: 21 fev. 2020.

BRASIL. **Portaria nº 3.389/MD**, de 21 de dezembro de 2012c. Política Cibernética de Defesa. Brasília, DF, 2012. Disponível em: http://www.lex.com.br/legis_24068327_

PORTARIA_NORMATIVA_N_3389_DE_21_DE_DEZEMBRO_DE_2012.aspx. Acesso em: 2 ago. 2020.

BRASIL. Presidência da República. **Decreto nº 10.222, de 5 de fevereiro de 2020.** Estratégia Nacional de Segurança Cibernética. Brasília, DF: Diário Oficial [da] República Federativa do Brasil, 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Decreto/D10222.htm. Acesso em: 10 abr. 2020.

BRASIL. Presidência da República. **Decreto nº 6.703, de 18 de dezembro de 2008.** Estratégia Nacional de Defesa. Publicado em: 19 dez. 2008. Brasília, DF: Diário Oficial [da] República Federativa do Brasil, 2008. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/decreto/d6703.htm. Acesso em: 23 jul. 2020.

CCDCOE. NATO Cooperative Cyber Defence Centre of Excellence. 2019. **Locked Shields.** Disponível em: https://ccdcoe.org/exercises/locked-shields/. Acesso em: 2 ago. 2020.

CLARKE, Richard A.; KNAKE, Robert K. **Guerra Cibernética:** A próxima ameaça à segurança e o que fazer a respeito. Rio de Janeiro: Brasport, 2015.

CORREIA, Henrique. Vários ataques no ciberespaço simulam capacidade de intervenção de várias entidades na região. Publicado em: 13/11/2019. **Funchal Notícias.** Disponível em: https://funchalnoticias.net/2019/11/13/varios-ataques-no-ciberespaco-simulam-capacidade-de-intervencao-de-varias-entidades-na-regiao/. Acesso em: 28 jul. 2020.

SHEVES, Shimon. Cyber 'War' Games Highlight Vital Security Flaws. Publicado em: 13 de março de 2017. **CyberTalk Blog.** Disponível em: https://www.cybertalkblog.co.uk/cyber-news-blog/cyber-war-games-highlight-vital-security-flaws/. Acesso em: 20 jul. 2020.

SILVA, Walbery Nogueira de Lima e. **Curso de Planejamento de Guerra Eletrônica e Guerra Cibernética em apoio às Operações:** Atuação colaborativa da Defesa Cibernética brasileira na proteção de infraestruturas críticas. 2019. 14 f. Ministério da Defesa. Exército Brasileiro. Comando de Comunicações e Guerra Eletrônica do Exército. Centro de Instrução de Guerra Eletrônica. Artigo Científico, Ministério da Defesa, Exército Brasileiro, Comando de Comunicações e Guerra Eletrônica do Exército - Centro de Instrução de Guerra Eletrônica. Brasília, DF, 2019. Disponível em: https://bdex.eb.mil.br/jspui/bitstream/123456789/4655/1/Artigo%20Cientifico%20%20TC%20Walbery%20-%20Atlz%2028%20OUT.pdf. Acesso em: 10 abr. 2020.

ANEXO — Níveis de decisão e Estrutura do SMDC

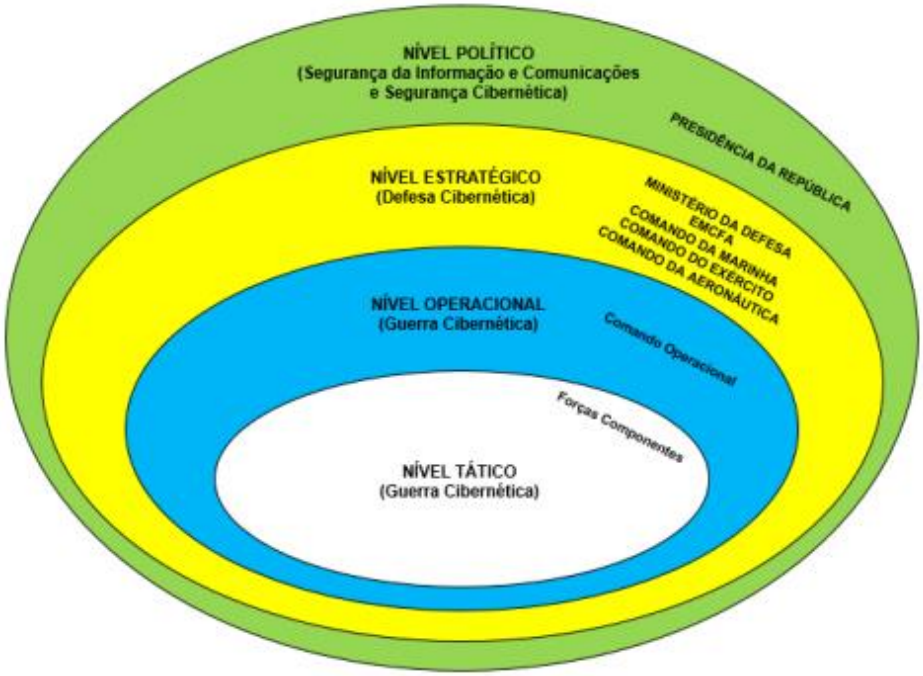

FIGURA 1 — Níveis de decisão.
Fonte: BRASIL, 2017b, p. 1-3.

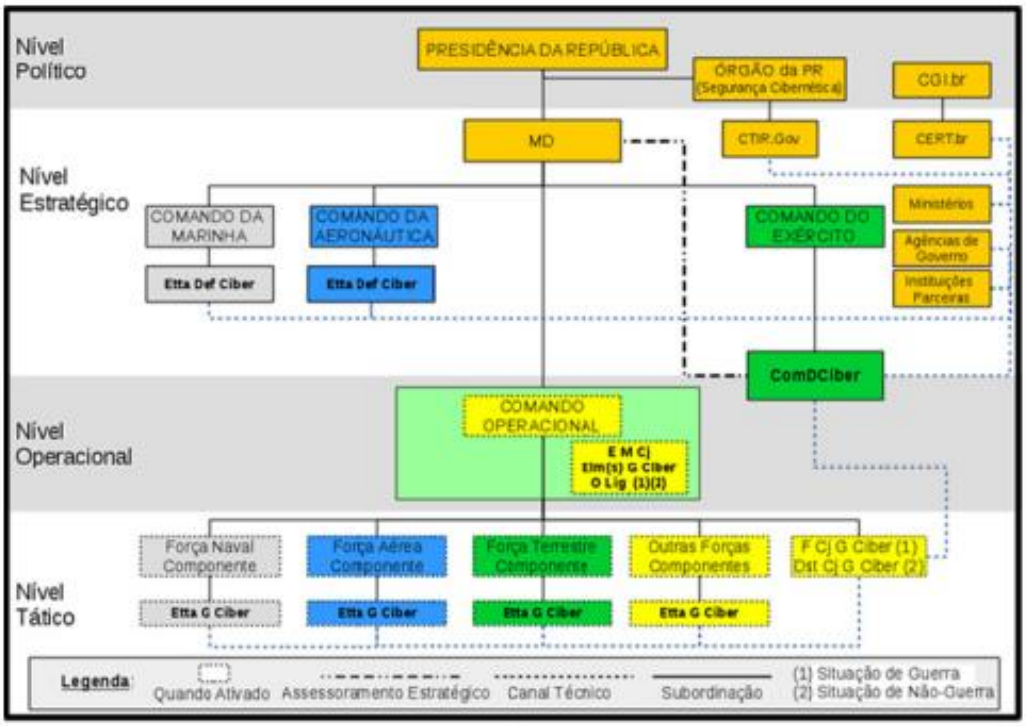

FIGURA 2 — Sistema Militar de Defesa Cibernética (SMDC).
Fonte: BRASIL, 2017b, p. 3-1.